

What Is Claimed Is:

1 1. An authenticated-encryption method that uses a key, a nonce and
2 an n-bit block cipher to encrypt a message into a ciphertext, the method
3 comprising:
4 partitioning the message into a message body comprising a sequence of n-
5 bit message blocks, and a message fragment of at most n bits;
6 generating a sequence of offsets from the nonce and the key;
7 computing a ciphertext body using the block cipher, the message body, the
8 key, the nonce, and the sequence of offsets;
9 computing a ciphertext fragment using the block cipher, the message
10 fragment, the key, and an offset;
11 computing a tag as a function of the message body, the message fragment,
12 the sequence of offsets, and the key; and
13 defining the ciphertext to include the ciphertext body, the ciphertext
14 fragment, and the tag.

1 2. The method of claim 1, wherein generating the sequence of offsets
2 involves:
3 determining a first offset as a function of the nonce and the key; and
4 determining each subsequent offset by combining a previous offset and a
5 basis offset, wherein each basis offset is determined as a function of the key.

1 3. The method of claim 1, wherein generating the sequence of offsets
2 involves determining an offset by combining a base offset and a fixed offset,
3 wherein the base offset is a function to the key and the nonce, and the fixed offset
4 is a function of the key and the position of the offset in a sequence of offsets.

1 4. The method of claim 1, wherein generating the sequence of offsets
2 involves:
3 generating a sequence of fixed offsets from the key;
4 generating a base offset from the key and the nonce;
5 generating a sequence of translated offsets by combining each fixed offset
6 with the base offset to get a corresponding translated offset; and
7 using the sequence of translated offsets as the sequence of offsets.

1 5. The method of claim 4, wherein the key determines a sequence of
2 basis offsets and each fixed offset is determined by xoring some combination of
3 basis offsets.

1 6. The method of claim 5, wherein each basis offset except for the
2 first basis offset is determined by a shift and a conditional xor applied to a
3 previous basis offset.

1 7. The method of claim 5, wherein the order that basis offsets are
2 combined into fixed offsets is determined according to a Gray code.

1 8. The method of claim 1, wherein generating the sequence of offsets
2 involves:
3 computing a sequence of basis offsets from the key;
4 computing a base offset from the key and the nonce; and
5 computing the first offset in the sequence of offsets as a function of the
6 base offset, the key, and the nonce, and computing each subsequent offset in the
7 sequence of offsets by combining the prior offset with a basis offset.

1 9. The method of claim 1, wherein generating the sequence of offsets
2 involves:
3 computing a key-variant by enciphering a constant with the block cipher,
4 wherein the block cipher is keyed by the given key; and
5 computing the sequence of offsets as a function of the key variant and the nonce.

1 10. The method of claim 1, wherein computing the ciphertext body
2 involves:
3 combining each message block in the message body with a corresponding
4 offset to produce a corresponding input block;
5 applying the block cipher to each input block to produce a corresponding
6 output block;
7 combining each output block with a corresponding offset to produce a
8 corresponding ciphertext block; and
9 concatenating the ciphertext blocks to determine the ciphertext body.

1 11. The method of claim 1, wherein computing the ciphertext fragment
2 involves:
3 computing a precursor pad as a function of an offset and the length of the
4 message;
5 computing a pad by applying the block cipher to the precursor pad; and
6 computing the ciphertext fragment by combining the message fragment
7 and the pad.

1 12. The method of claim 1, wherein computing the tag involves:
2 computing a checksum as a function of the message, the ciphertext
3 fragment, and the sequence of offsets; and
4 computing the tag as a function of the checksum, the key, and an offset.

1 13. The method of claim 1, wherein computing the tag involves:
 2 computing a checksum from at least the message ;
 3 combining the checksum with an offset to produce a precursor full tag;
 4 computing a full tag by applying the block cipher to the precursor full tag;
 5 and
 6 computing a tag as a portion of the full tag.

1 14. An authenticated-encryption method that uses a key, a nonce, and
 2 an n-bit block cipher to decrypt a ciphertext into a message or a message-invalid
 3 signal, the method comprising:
 4 partitioning the ciphertext into a ciphertext body comprising a sequence of
 5 n-bit ciphertext blocks, a ciphertext fragment of at most n bits, and a tag;
 6 generating a sequence of offsets from the nonce and the key;
 7 computing a message body using the block cipher, the ciphertext body, the
 8 key, the nonce, and the sequence of offsets;
 9 computing a message fragment using the block cipher, the ciphertext
 10 fragment, the key, and an offset;
 11 computing a new tag as a function of the message body, the message
 12 fragment, the sequence of offsets, the block cipher, and the key; and
 13 comparing the new tag with the tag;
 14 if the new tag matches the tag, returning the message, wherein the
 15 message includes the message body and the message fragment; and
 16 if the new tag does not match the tag, returning a message-invalid signal.

1 15. The method of claim 14, wherein generating the sequence of
 2 offsets involves:
 3 generating a sequence of fixed offsets from the key;

4 generating a base offset from the key and the nonce;
5 generating a sequence of translated offsets by combining each fixed offset
6 with the base offset to get a corresponding translated offset; and
7 using the sequence of translated offsets as the sequence of offsets.

1 16. The method of claim 14, wherein computing the message body
2 involves:

3 combining each ciphertext block in the ciphertext body with a
4 corresponding offset to produce a corresponding output block;
5 applying the block-cipher inverse to each output block to produce a
6 corresponding input block;
7 combining each input block with a corresponding offset to produce a
8 corresponding message block; and
9 defining the message body to be the sequence of message blocks.

1 17. The method of claim 14, wherein computing the message fragment
2 involves:

3 computing a precursor pad as a function of an offset and the length of the
4 ciphertext;
5 computing a pad by applying the block cipher to the precursor pad; and
6 computing the message fragment by combining the ciphertext fragment
7 and the pad.

1 18. The method of claim 14, wherein computing the tag involves:
2 computing a checksum as a function of at least the message; and
3 computing the tag as a function of the checksum, the key, and an offset.

1 19. A computer-readable storage medium storing instructions that

2 when executed by a computer cause the computer to perform an authenticated-
 3 encryption method that uses a key and a nonce to encrypt a message into a
 4 ciphertext, the method comprising:
 5 partitioning the message into a message body including a sequence of n-
 6 bit message blocks, and a message fragment of at most n bits;
 7 generating a sequence of offsets from the nonce and the key;
 8 computing a ciphertext body using a block cipher, the message body, the
 9 key, the nonce, and the sequence of offsets;
 10 computing a ciphertext fragment using the block cipher, the message
 11 fragment, the key, and an offset;
 12 computing a tag as a function of the message body, the message fragment,
 13 the sequence of offsets, and the key; and
 14 defining the ciphertext to include the ciphertext body, the ciphertext
 15 fragment, and the tag.

1 20. The computer-readable storage medium of claim 19, wherein
 2 generating the sequence of offsets involves:
 3 determining a first offset as a function of the nonce and the key; and
 4 determining each subsequent offset by combining a previous offset and a
 5 basis offset, wherein each basis offset is determined as a function of the key.

1 21. The computer-readable storage medium of claim 19, wherein
 2 generating the sequence of offsets involves determining an offset by combining a
 3 base offset and a fixed offset, wherein the base offset is a function to the key and
 4 the nonce, and the fixed offset is a function of the key and a position of the fixed
 5 offset in a sequence of fixed offsets.

1 22. The computer-readable storage medium of claim 19, wherein
2 generating the sequence of offsets involves:
3 generating a sequence of fixed offsets from the key;
4 generating a base offset from the key and the nonce;
5 generating a sequence of translated offsets by combining each fixed offset
6 with the base offset to get a corresponding translated offset; and
7 using the sequence of translated offsets as the sequence of offsets.

1 23. The computer-readable storage medium of claim 22, wherein the
2 key determines a sequence of basis offsets and each fixed offset is determined by
3 xoring some combination of basis offsets.

1 24. The computer-readable storage medium of claim 23, wherein each
2 basis offset except for the first basis offset is determined by a shift and a
3 conditional xor applied to a previous basis offset.

1 25. The computer-readable storage medium of claim 24, wherein the
2 order that basis offsets are combined into fixed offsets is determined according to
3 a Gray code.

1 26. The computer-readable storage medium of claim 19, wherein
2 generating the sequence of offsets involves:
3 computing a sequence of basis offsets from the key;
4 computing a base offset from the key and the nonce; and
5 computing a sequence of translated offsets, wherein the first offset is
6 determined from the base offset, the key, and the nonce, and subsequent offsets
7 are determined by combining the prior translated offset with a basis offset.

1 27. The computer-readable storage medium of claim 19, wherein
2 generating the sequence of offsets involves:
3 computing a key-variant offset by enciphering a constant with the block
4 cipher, wherein the block cipher is keyed by a given key; and
5 computing the sequence of offsets using the key-variant offset.

1 28. The computer-readable storage medium of claim 19, wherein
2 computing the ciphertext body involves:
3 combining each message block in the message body with a corresponding
4 offset to produce a corresponding input block;
5 applying the block cipher to each input block to produce a corresponding
6 output block; and
7 combining each output block with a corresponding offset to produce a
8 corresponding ciphertext block.

1 29. The computer-readable storage medium of claim 19, wherein
2 computing the ciphertext fragment involves:
3 computing a precursor pad as a function of an offset;
4 computing a pad by applying the block cipher to the precursor pad; and
5 computing the ciphertext fragment by combining the message fragment
6 and the pad.

1 30. The computer-readable storage medium of claim 19, wherein
2 computing the tag involves:
3 computing a checksum as a function of the message and a sequence of
4 offsets; and
5 computing the tag as a function of the checksum, the key, and an offset.

1 31. The computer-readable storage medium of claim 19, wherein
 2 computing the tag involves:
 3 computing a checksum from the message blocks, the message fragment,
 4 and a pad;
 5 combining the checksum with an offset to produce a precursor full tag;
 6 computing a full tag by applying the block cipher to the precursor full tag;
 7 and
 8 computing a tag as a portion of the full tag.

1 32. A computer-readable storage medium storing instructions that
 2 when executed by a computer cause the computer to perform an authenticated-
 3 encryption method that uses a key and a nonce to decrypt a ciphertext into a
 4 message, the method comprising:
 5 partitioning the ciphertext into a ciphertext body including a sequence of
 6 n-bit ciphertext blocks, a ciphertext fragment of at most n bits, and a tag;
 7 generating a sequence of offsets from the nonce and the key;
 8 computing a message body using a block cipher, the ciphertext body, the
 9 key, the nonce, and the sequence of offsets;
 10 computing a message fragment using the block cipher, the ciphertext
 11 fragment, the key, and an offset;
 12 computing a new tag as a function of the message body; and
 13 comparing the new tag with the tag;
 14 if the new tag matches the tag, returning the message, wherein the
 15 message includes the message body and the message fragment; and
 16 otherwise, if the new tag does not match the tag, returning a message
 17 invalid signal.

1 33. The computer-readable storage medium of claim 32, wherein
2 generating the sequence of offsets involves:
3 generating a sequence of fixed offsets from the key;
4 generating a base offset from the key and the nonce;
5 generating a sequence of translated offsets by combining each fixed offset
6 with the base offset to get a corresponding translated offset; and
7 using the sequence of translated offsets as the sequence of offsets.

1 34. The computer-readable storage medium of claim 32, wherein
2 computing the message body involves:
3 combining each ciphertext block in the ciphertext body with a
4 corresponding offset to produce a corresponding input block;
5 applying the block cipher to each input block to produce a corresponding
6 output block; and
7 combining each output block with a corresponding offset to produce a
8 corresponding message block.

1 35. The computer-readable storage medium of claim 32, wherein
2 computing the message fragment involves:
3 computing a precursor pad as a function of an offset;
4 computing a pad by applying the block cipher to the precursor pad; and
5 computing the message fragment by combining the ciphertext fragment
6 and the pad.

1 36. The computer-readable storage medium of claim 32, wherein
2 computing the tag involves:
3 computing a checksum as a function of the message body; and
4 computing the tag as a function of the checksum, the key, and an offset.

37. An authenticated-encryption apparatus that uses a key and a nonce to encrypt a message into a ciphertext, the apparatus comprising:

a partitioning mechanism that is configured to partition the message into a message body including a sequence of n-bit message blocks, and a message fragment of at most n bits;

an offset generating mechanism that is configured to generate a sequence of offsets from the nonce and the key;

an enciphering mechanism that is configured to compute a ciphertext body using a block cipher, the message body, the key, the nonce, and the sequence of offsets;

wherein the enciphering mechanism is additionally configured to compute a ciphertext fragment using the block cipher, the message fragment, the key, and an offset;

a tag computing mechanism that is configured to compute a tag as a function of the message body, the message fragment, the sequence of offsets, and the key; and

an assembly mechanism that is configured to define the ciphertext to include the ciphertext body, the ciphertext fragment, and the tag.

38. An authenticated-encryption apparatus that uses a key and a nonce to decrypt a ciphertext into a message, the apparatus comprising:

a partitioning mechanism that is configured to partition the ciphertext into a ciphertext body including a sequence of n-bit ciphertext blocks, a ciphertext fragment of at most n bits, and a tag;

an offset generating mechanism that is configured to generate a sequence of offsets from the nonce and the key;

a deciphering mechanism that is configured to compute a message body

9 using a block cipher, the ciphertext body, the key, the nonce, and the sequence of
 10 offsets;
 11 wherein the deciphering mechanism is configured to compute a message
 12 fragment using the block cipher, the ciphertext fragment, the key, and an offset;
 13 a tag computing mechanism that is configured to compute a new tag as a
 14 function of the message body; and
 15 a comparison mechanism that is configured to compare the new tag with
 16 the tag;
 17 wherein if the new tag matches the tag, the apparatus is configured to
 18 return the message, wherein the message includes the message body and the
 19 message fragment; and
 20 wherein if the new tag does not match the tag, the apparatus is configured
 21 to return a message invalid signal.

1 39. An authenticated-encryption method that uses an n-bit block cipher, a key,
 2 and an n-bit nonce to encrypt a message into a ciphertext, the method comprising:
 3 partitioning the message into m message blocks and one final fragment,
 4 each message block having n bits and the final fragment having between 0 and n
 5 bits;
 6 using the block cipher, the key, and the nonce to generate a sequence of m
 7 offsets, each offset having n bits;
 8 using the block cipher, the key, the nonce, and the length of the message
 9 to generate an n-bit final offset;
 10 for each number i between 1 and m, xoring the i^{th} message block with the
 11 i^{th} offset to determine an i^{th} input block;
 12 for each number i between 1 and m, applying the block cipher, keyed by
 13 the key, to the i^{th} input block, to determine an i^{th} output block;
 14 for each number i between 1 and m, xoring the i^{th} output block with the i^{th}

15 offset to determine an i^{th} ciphertext block;
 16 concatenating the m ciphertext blocks to determine a ciphertext body;
 17 computing an encoded length by encoding the length of the final fragment
 18 as an n -bit string;
 19 xoring the encoded length with the final offset to determine a precursor
 20 pad;
 21 computing a pad by applying the block cipher, keyed by the key, to the
 22 precursor pad;
 23 xoring the final fragment with a portion of the pad to determine a
 24 ciphertext fragment having the same length as the final fragment;
 25 computing a padded ciphertext fragment by appending to the ciphertext
 26 fragment a sufficient number of zero bits so that the padded ciphertext fragment
 27 has n bits;
 28 computing a checksum by xoring together the m message blocks, the pad,
 29 and the padded ciphertext fragment;
 30 computing a precursor full tag by xoring together the checksum and the
 31 m^{th} offset;
 32 determining a full tag by applying the block cipher, keyed by the key, to
 33 the precursor full tag;
 34 computing a tag as a portion of the full tag; and
 35 defining the ciphertext to be the ciphertext body, the ciphertext fragment,
 36 and the tag.

1 40. The method of claim 39, wherein the i^{th} offset from the sequence of offsets
 2 is determined by:
 3 computing a 0^{th} basis offset by applying the block cipher, keyed by the
 4 key, to a constant;

5 for each positive number i , defining the i^{th} basis offset from the prior basis
6 offset by shifting the prior basis offset left one position, and then xoring the
7 resulting value with a constant that depends on the first bit of the prior basis
8 offset;
9 computing a base offset by applying the block cipher, keyed by the key, to
10 the xor of the 0^{th} basis offset and the nonce;
11 defining the first offset in the sequence of offsets as the xor of the 0^{th} basis
12 offset and the base offset; and
13 for each integer i greater than one, defining the i^{th} offset in the sequence of
14 offsets as the xor of the prior offset and the j^{th} basis offset, where j is the number
15 of zero-bits following the last one-bit when the number i is written in binary.

1 41. The method of claim 39, wherein the final offset is determined by
2 shifting the 0^{th} basis offset one position to the right, xoring a constant that
3 depends on the last bit of the 0^{th} basis offset, and then xoring the m^{th} offset.

1 42. An authenticated-encryption method that encrypts a message using
2 a key, and a nonce, said method involving the computation of a sequence of
3 offsets, wherein this sequence of offsets is determined by:
4 computing a 0^{th} basis offset as a function of the key;
5 for each positive number i , defining the i^{th} basis offset from the prior basis
6 offset by shifting the prior basis offset by one position and then xoring a constant
7 that depends on a given bit of the prior basis offset;
8 computing a base offset as a function of at least the nonce;
9 defining the 1^{st} offset in the sequence of offsets as a function of a basis
10 offset and the base offset; and

11 for each integer i greater than one, defining the i^{th} offset in the sequence
12 of offsets as the xor of the prior offset and a basis offset associated to the number
13 i .

1 43. The method of claim 42 wherein the basis offset associated to the
2 number i is the j^{th} basis offset, where j is the number of zero-bits following the
3 last one-bit when the number i is written in binary.

1 44. An authenticated-encryption method that encrypts a message into a
2 ciphertext using a key and a nonce, comprising:
3 computing a sequence of basis offsets from the key;
4 computing a base offset from the key and the nonce;
5 computing a sequence of offsets, where the first offset is determined
6 from the base offset, the key, and the nonce, and each subsequent offset is
7 determined by combining the prior offset and a basis offset; and
8 computing the ciphertext from at least the message, the key, and the
9 sequence of offsets.

1 45. An authenticated-encryption method that encrypts a message using
2 an n -bit block cipher, a key and a nonce, said method involving the computation
3 of a sequence of n -bit offsets, where computing the sequence of offsets involves:
4 fixing a positive n -bit constant, where 2^n minus this constant is prime;
5 computing an n -bit stride using the key and possibly the nonce;
6 computing a first offset using the key and the nonce; and
7 computing each subsequent offset by n -bit computer addition of the prior
8 offset and the stride, and further followed by computer addition of the said
9 constant whenever the first addition resulted in a carry.

1 46. The method of claim 45, wherein the specified constant is the
2 smallest number such that 2^n minus this number is prime.

1 47. An authenticated-encryption method that encrypts a message using
2 a nonce and a block cipher keyed by a given key, comprising:
3 computing a key-variant by enciphering a constant with the keyed block
4 cipher;
5 computing a sequence of offsets using the key variant and the nonce; and
6 computing the ciphertext using at least the keyed block cipher, the
7 message, and the sequence of offsets.

1 48. An authenticated-encryption method that encrypts a message using
2 a nonce and a block cipher keyed by a given key, comprising:
3 computing a key-variant by enciphering a constant with the keyed block
4 cipher;
5 computing a sequence of basis offsets as a function of the key-variant;
6 computing a base offset using at least the nonce;
7 computing a 1st offset from a basis offset and the base offset;
8 for each number i greater than 1, computing the i^{th} offset in the sequence
9 of offsets by combining the prior offset and a basis offset; and
10 computing the ciphertext using at least the keyed block cipher, the
11 message, and the sequence of offsets.

1 49. The method of claim 48, wherein each basis offset except for the
2 first basis offset is determined by shifting the prior basis offset by one position
3 and then xoring a constant that depends on a given bit of the prior basis offset.

1 50. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform an authenticated-
3 encryption method that uses an n-bit block cipher, a key, and an n-bit nonce to
4 encrypt a message into a ciphertext, the method comprising:
5 partitioning the message into m message blocks and one final fragment,
6 each message block having n bits and the final fragment having between 0 and n
7 bits;
8 using the block cipher, the key, and the nonce to generate a sequence of m
9 offsets, each offset having n bits;
10 using the block cipher, the key, the nonce, and the length of the message
11 to generate an n-bit final offset;
12 for each number i between 1 and m, xoring the ith message block with the
13 ith offset to determine an ith input block;
14 for each number i between 1 and m, applying the block cipher, keyed by
15 the key, to the ith input block, to determine an ith output block;
16 for each number i between 1 and m, xoring the ith output block with the ith
17 offset to determine an ith ciphertext block;
18 concatenating the m ciphertext blocks to determine a ciphertext body;
19 computing an encoded length by encoding the length of the final fragment
20 as an n-bit string;
21 xoring the encoded length with the final offset to determine a precursor
22 pad;
23 computing a pad by applying the block cipher, keyed by the key, to the
24 precursor pad;
25 xoring the final fragment with a portion of the pad to determine a
26 ciphertext fragment having the same length as the final fragment;
27 computing a padded ciphertext fragment by appending to the ciphertext
28 fragment a sufficient number of zero bits so that the padded ciphertext fragment

29 has n bits;
 30 computing a checksum by xoring together the m message blocks, the pad,
 31 and the padded ciphertext fragment;
 32 computing a precursor full tag by xoring together the checksum and the
 33 m^{th} offset;
 34 determining a full tag by applying the block cipher, keyed by the key, to
 35 the precursor full tag;
 36 computing a tag as a portion of the full tag; and
 37 defining the ciphertext to be the ciphertext body, the ciphertext fragment,
 38 and the tag.

1 51. The computer-readable storage medium of claim 50, wherein the
 2 i^{th} offset from the sequence of offsets is determined by:
 3 computing a 0^{th} basis offset by applying the block cipher, keyed by the
 4 key, to a constant;
 5 for each positive number i, defining the i^{th} basis offset from the prior basis
 6 offset by shifting the prior basis offset left one position, and then xoring the
 7 resulting value with a constant that depends on the first bit of the prior basis
 8 offset;
 9 computing a base offset by applying the block cipher, keyed by the key, to
 10 the xor of the 0^{th} basis offset and the nonce;
 11 defining the first offset in the sequence of offsets as the xor of the 0^{th} basis
 12 offset and the base offset; and
 13 for each integer i greater than one, defining the i^{th} offset in the sequence of
 14 offsets as the xor of the prior offset and the j^{th} basis offset, where j is the number
 15 of zero-bits following the last one-bit when the number i is written in binary.

3 encryption method that encrypts a message into a ciphertext using a key and a
4 nonce, the method comprising:
5 computing a sequence of basis offsets from the key;
6 computing a base offset from the key and the nonce;
7 computing a sequence of offsets, where the first offset is determined
8 from the base offset, the key, and the nonce, and each subsequent offset is
9 determined by combining the prior offset and a basis offset; and
10 computing the ciphertext from at least the message, the key, and the
11 sequence of offsets.

1 56. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform an authenticated-
3 encryption method that encrypts a message using an n-bit block cipher, a key and a
4 nonce, said method involving the computation of a sequence of n-bit offsets,
5 where computing the sequence of offsets involves:
6 fixing a positive n-bit constant such that 2^n minus this constant is prime;
7 computing an n-bit stride using the key and possibly the nonce;
8 computing a first offset using the key and the nonce; and
9 computing each subsequent offset by n-bit computer addition of the prior
10 offset and the stride, and further followed by computer addition of the said
11 constant whenever the first addition resulted in a carry.

1 57. The computer-readable storage medium of claim 56, wherein the
2 specified constant is the smallest number such that 2^n minus this number is prime.

1 58. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform an authenticated-

2 n-bit block cipher, a key, and an n-bit nonce to encrypt a message into a
3 ciphertext, comprising:
4 a partitioning mechanism that is configured to partition the message into
5 m message blocks and one final fragment, each message block having n bits and
6 the final fragment having between 0 and n bits;
7 an offset-generating mechanism that is configured to,
8 use the block cipher, the key, and the nonce to generate a
9 sequence of m offsets, each offset having n bits, and to
10 use the block cipher, the key, the nonce, and the length of
11 the message to generate an n-bit final offset;
12 an xoring mechanism, wherein for each number i between 1 and m, the
13 xoring mechanism is configured to xor the i^{th} message block with the i^{th} offset to
14 determine an i^{th} input block;
15 an enciphering mechanism, wherein for each number i between 1 and m,
16 the enciphering mechanism is configured to apply the block cipher, keyed by the
17 key, to the i^{th} input block, to determine an i^{th} output block;
18 wherein for each number i between 1 and m, the xoring mechanism is
19 configured to xor the i^{th} output block with the i^{th} offset to determine an i^{th}
20 ciphertext block;
21 a concatenating mechanism that is configured to concatenate the m
22 ciphertext blocks to determine a ciphertext body;
23 a computing mechanism that is configured to compute an encoded length
24 by encoding the length of the final fragment as an n-bit string;
25 wherein the xoring mechanism is configured to xor the encoded length
26 with the final offset to determine a precursor pad;
27 wherein the computing mechanism is configured to compute a pad by
28 applying the block cipher, keyed by the key, to the precursor pad;
29 wherein the xoring mechanism is configured to xor the final fragment with

```

30  a portion of the pad to determine a ciphertext fragment having the same length as
31  the final fragment;

```

32 wherein the computing mechanism is configured to compute a padded
33 ciphertext fragment by appending to the ciphertext fragment a sufficient number
34 of zero bits so that the padded ciphertext fragment has n bits;

35 wherein the computing mechanism is configured to compute a checksum
36 by xoring together the m message blocks, the pad, and the padded ciphertext
37 fragment;

38 wherein the computing mechanism is configured to compute a precursor
39 full tag by xoring together the checksum and the mth offset;

40 wherein the computing mechanism is configured to determine a full tag by
41 applying the block cipher, keyed by the key, to the precursor full tag;

42 wherein the computing mechanism is configured to compute a tag as a
43 portion of the full tag; and

44 a defining mechanism that is configured to define the ciphertext to be the
45 ciphertext body, the ciphertext fragment, and the tag.

1 62. An authenticated-encryption apparatus that encrypts a message
2 using a key, and a nonce, said method involving the computation of a sequence of
3 offsets, comprising:

4 an offset computing mechanism that is configured to compute a 0th basis
5 offset as a function of the key;

6 wherein for each positive number i, the offset computing mechanism is
7 configured to define the i^{th} basis offset from the prior basis offset by shifting the
8 prior basis offset by one position and then xoring a constant that depends on a
9 given bit of the prior basis offset;

10 wherein the offset computing mechanism is configured to compute a base
11 offset as a function of at least the nonce;

12 wherein the offset computing mechanism is configured to define the 1st
13 offset in the sequence of offsets as a function of a basis offset and the base offset;
14 and
15 wherein for each integer i greater than one, the offset computing
16 mechanism is configured to define the i^{th} offset in the sequence of offsets as the
17 xor of the prior offset and a basis offset associated to the number i .

1 63. An authenticated-encryption apparatus that encrypts a message
2 into a ciphertext using a key and a nonce, comprising a computing mechanism
3 that is configured to:

4 compute a sequence of basis offsets from the key;
5 compute a base offset from the key and the nonce;
6 compute a sequence of offsets, where the first offset is determined
7 from the base offset, the key, and the nonce, and each subsequent offset is
8 determined by combining the prior offset and a basis offset; and to
9 compute the ciphertext from at least the message, the key, and the
10 sequence of offsets.

1 64. An authenticated-encryption apparatus that encrypts a message
2 using an n -bit block cipher, a key and a nonce, comprising:
3 an offset computing mechanism that is configured to compute a sequence
4 of n -bit offsets, by

5 fixing a positive n -bit constant, where 2^n minus this
6 constant is prime;
7 computing an n -bit stride using the key and possibly the
8 nonce;
9 computing a first offset using the key and the nonce; and
10 computing each subsequent offset by n -bit computer

11 addition of the prior offset and the stride, and further followed by
 12 computer addition of the said constant whenever the first addition
 13 resulted in a carry.

1 65. An authenticated-encryption apparatus that encrypts a message
 2 using a nonce and a block cipher keyed by a given key, comprising a computing
 3 mechanism that is configured to:
 4 compute a key-variant by enciphering a constant with the keyed block
 5 cipher;
 6 compute a sequence of offsets using the key variant and the nonce; and to
 7 compute the ciphertext using at least the keyed block cipher, the message,
 8 and the sequence of offsets.

1 66. An authenticated-encryption apparatus that encrypts a message
 2 using a nonce and a block cipher keyed by a given key, comprising a computing
 3 mechanism that is configured to:
 4 compute a key-variant by enciphering a constant with the keyed block
 5 cipher;
 6 compute a sequence of basis offsets as a function of the key-variant;
 7 compute a base offset using at least the nonce;
 8 compute a 1st offset from a basis offset and the base offset;
 9 for each number i greater than 1, to compute the ith offset in the sequence
 10 of offsets by combining the prior offset and a basis offset; and to
 11 compute the ciphertext using at least the keyed block cipher, the message,
 12 and the sequence of offsets.